UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,878	08/18/2003	Jagdeep Singh Sahota	124517-00701 (07035632)	3312

65357 7590 01/11/2008

Quarles & Brady LLP
TWO NORTH CENTRAL AVENUE
One Renaissance Square
PHOENIX, AZ 85004-2391

EXAMINER	
SHUMATE, PAUL W	
ART UNIT	**PAPER NUMBER**
3693	

MAIL DATE	DELIVERY MODE
01/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/642,878	SAHOTA ET AL.	
	Examiner	Art Unit	
	Paul Shumate	3694	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-28 and 39-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-28 and 39-48* is/are rejected.

7)☒ Claim(s) *44 and 45* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims and Acknowledgement of Applicant's Election

1. This action is in reply to the Application filed on 01/02/2008. Claims 14-28 and 39-48 have been examined and are currently pending. Original claims 14-28 (Invention II) have been elected without traverse as per Applicant's response filed on 01/02/2008 by attorney Bradley K. DeSandro. Claims 1-13 and 29-38 have been cancelled and are therefore withdrawn from consideration. Claims 39-48, including both claim 44s and both claim 45s, have been added. Applicant submits that the added claims 39-44 fall within the elected invention, Group II.

Claim Objections

2. Claims 44 and 45 objected to because of the following informalities: There are two claim 44s and two claim 45s. The second claim 44 is found after claim 48. Claim numbers should be sequential, in the order that the claims appear in the disclosure. The examiner suggests renumbering claims 44, 44, 45, 45, 46, 47, and 48. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 26 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 26 recites the limitation "said first verification value" in line 1. There is insufficient antecedent basis for this limitation in the claim.

5. Claims 39, 40, 41, 43, 44 (first), 44 (second), 45 (first), 45 (second), 47, and 48 are rejected under 35 U.S.C. 112, second paragraph, as such claim is directed to neither a process nor a machine, but rather embraces and/or overlaps two different statutory classes of invention which has deemed ambiguous under 35 U.S.C. 112. This section requires a claim to particularly point out and distinctly claim the subject matter which the appellant regards as his invention. However, the "invention" referred to in the second paragraph of 35 USC 112 is also subject to the requirements of 35 USC 101. This section of the statute requires that in order to be patentable the invention must be a "new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." A claim intended to embrace or overlap two different statutory classes of invention set forth in 35 USC 101 is precluded by the express language of 35 USC 101 which is drafted so as to set forth the statutory classes of invention in the alternative only. A single claim which purposes to be both a product or machine and a process is ambiguous and is properly rejected under 35 USC 112, second paragraph, for failing to particularly point out and distinctly claim the invention. Ex parte Lyell, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 39, 40, 41, 43, 44 (first), 44 (second), 45 (first), 45 (second), 47, and 48 rejected under 35 U.S.C. 101 because the claimed invention is directed to neither a process, a machine, a manufacture, nor a composition of matter, but rather embraces and/or overlaps multiple statutory classes of invention which 35 U.S.C. 101 is designed to prevent. In Ex parte Lyell, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim(s) 14-19, 25, 27, 28, and 39-48 rejected under 35 U.S.C. 103(a) as being unpatentable over Li, U.S. Patent Application Publication No.: 2002/0153424 in view of Buer, U.S. Patent No.: 5,835,599.

> Examiner's Note: The Examiner has cited particular columns and line numbers in the references as applied to the claims for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.
>
> Independent claims are examined together, since they are not patentable distinct. If applicant expressly states on the record that two or more independent and distinct inventions are claimed in a single application, the Examiner may require the applicant to elect an invention to which the claims will be restricted.

As per claims 14, 42, 46, Li teaches a processor-implemented method of dynamically creating a verification value for a transaction (see at least paragraph(s) 0007) comprising: creating, in response to the transaction involving a payment device, a base record having a first data value and a second data value (see at least paragraph(s) 0009). Li teaches that the creation of the dynamic digital certificate (verification value) is a function of a first group of variables and a second group of variables. The first group comprises the internally stored credit card account number, the card issuing date and time, and the card expiration date. The second group comprises dynamic data such as the instant date and time at which the transaction is taking place (see at least paragraph(s) 0009, 0024).

While Li does teach a symmetric encryption authentication method and system (see at least paragraph(s) 0007, 0012, 0020) that runs an encryption algorithm on plaintext data, which is formed from

both the internally stored and the dynamic data, to produce a dynamic digital certificate that is compared against an independently created authentication code created by the authentication system, Li does not explicitly disclose the encryption steps of: splitting the base record into a first field and a second field; encrypting the first field using a first encryption key; performing an exclusive-OR (XOR) operation on the encrypted first field and the second field to produce a first result; encrypting the first result using a second encryption key to produce a second result; decrypting the second result using a decryption key to produce a third result; encrypting the third result using a third encryption key to produce a fourth result; sequentially extracting each value between 0 and 9 from the most-significant digit to the least-significant digit of the fourth result to produce a fifth result; sequentially extracting and subtracting hexadecimal A from each value between hexadecimal A and hexadecimal F from the most-significant digit to the least-significant digit of the fourth result to produce the sixth result; concatenating the fifth result and the sixth result to produce a seventh result; selecting one or more values from the seventh result as a verification value for the transaction.

Buer, however, teaches splitting plaintext into 64-bit blocks P1 and P2 (see at least column 1 lines 57-59, column 2 lines 7-8, column 4 lines 26-32, and column 5 lines 48-50) encrypting blocks with an encryption key (see at least column 4 lines 1-4 and column 4 lines 36-40) performing an XOR operation on an unencrypted (plaintext) block and on an encrypted (ciphertext) block (see at least column 4 lines 20-22, column 4 lines 46-48, and column 5 lines 7-10) and encrypting encrypted results iteratively blocks (see at least column 4 lines 36-40). Buer notes that his teachings contemplate using different combinations and numbers of cipher stages, feedback paths, and output taps (see at least column 3 lines 3-6). Buer further teaches that decryption can be done with the same principle architecture used for encryption (see at least column 5 lines 5-6 and column 6 lines 58-60) and that decryption is the act of returning encrypted data back into its original form (see at least column 1 lines 14-15). Because the method is still in the process of creating an *encrypted* verification value, and because a decryption step that doesn't result in a decrypted (original form) value is substantially the same as an encryption step, the step of decrypting the second result using a decryption key to produce a third result is interpreted to be

equivalent to encrypting the second result using an encryption key to produce a third result, and is therefore taught by Buer in at least column 3 lines 3-6 and column 4 lines 36-40. Buer further teaches extracting, rearranging, and manipulating data blocks using substitutions in conjunction with permutations (see at least column 5 lines 45-47), expansion permutations (see at least column 5 lines 55-64), transformations, circular shifts, compression permutations (see at least column 6 lines 1-11), S-box substitutions, P-box permutations (see at least column 6 lines 17-32), and concatenation to produce a final encoded value (see at least column 4 lines 13-14).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to have incorporated the steps taught by Buer into the teachings of Li because all these steps are old and well known in the art and different combinations and numbers of cipher stages, feedback paths, and output tags are employed routinely in many different strategies and methods for data encryption depending on the desired ratio of security to encryption/decryption speed (see at least column 1 lines 32-35, column 2 lines 11-19, and column 3 lines 3-6).

As per claims 15, 16, 17, 18, Buer further teaches using equivalent first, second, and third encryption keys (see at least column 1 lines 57-59, column 3 lines 13-14, column 3 lines 56-59, column 4 lines 1-2, and column 4 lines 36-40) using different encryption/decryption keys (see at least column 6 lines 11-13, column 7 lines 31-34, and column 8 lines 13-16) and that the base record is 128-bits in length (see at least column 4 lines 26-32).

As per claims 19 Li further teaches the first data value comprises: a primary account number for the payment service (see at least paragraph(s) 0008, 0009, 0020)

As per claim 25, Li further teaches the second data value comprises a value derived from the payment data (see at least paragraph(s) 0009, 0024). Li teaches using the instant date and time at which a transaction is being processed as the dynamic part of the data on which the dynamic digital certificate is partially based.

As per claim 27, Buer further teaches padding data to a predetermined length (see at least column 4 lines 8-11)

As per claim 28, Li teaches that the dynamic digital certificate is created by an encryption algorithm on the card. The certificate is a function of variables including both data stored on the card and current transaction data. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to base the encryption keys on data stored on the card because this minimizes the chance of fraud because it would be nearly impossible for anyone other than the card issuer or the card itself to replicate the encryption algorithm.

Regarding claims 39, 40, 41, 43, 44 (first), 44 (second), 45 (first), 45 (second), 47, and 48, Li further teaches a smart "SecuAll Card" with a complete micro computer system implanted in the card used for conducting secure credit card transactions using dynamic digital certificates generated by both the SecuAll Card and a third party authenticating service at the time of a transaction. Upon approval by an authentication server, payment can be issued against the customers credit card account. This card can incorporate many cards or just one card, and it can be set up to work with big name credit services such as Visa, MasterCard, Discover, and American Express (see at least paragraph(s) 0002, 0007-0009, 0011, 0020). Li also teaches that the transaction method and system can be used by smart cards, electronic cards, cell phones, regular phones, PDAs, two-way pagers, and computers.

10. Claim(s) , 21, 22, 23, 24, and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Li, in view of Buer, further in view of Official Notice.

As per claims 20, 21, 22, 23, 24, and 26, the examiner takes Official Notice that the limitations added by these claims are old and well known in the art of digital transaction verification and encryption. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to base an encrypted transaction verification value on unique identifier variables and/or other personalized variables such as digital signatures, transaction counters, or cryptograms because these values would only be known by the card issuer and the card device itself which reduces the chance of fraud in credit card transactions (see at least paragraph(s) 0006 in Li).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Shumate whose telephone number is 571-270-1830. The examiner can normally be reached on M-F 8:30 AM - 6:00 PM, EST alt Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Kramer can be reached on 571-272-6783. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Name: Paul W. Shumate
Title: Patent Examiner
Date: 01/07/08
Signature:

1/7/08

JAMES A. KRAMER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600